JOURNAL OF ALGEBRA 74, 535–542 (1982)

Der Liftungsindex primitiver Galoisdarstellungen

HANS OPOLKA

Mathematisches Institut, Roxeler Strasse 64, D-4400 Münster, West Germany

Communicated by B. Huppert

Received June 2, 1981

1. EINLEITUNG

Sei k ein Zahlkörper und sei $G_k = G(\bar{k}/k)$ die absolute Galoisgruppe von k. Nachdem durch die abelsche Klassenkörpertheorie eine Beschreibung der eindimensionalen stetigen Darstellungen von G_k und deren L-Reihen gelungen ist, interessiert man sich seit einiger Zeit nummehr auch für die höherdimensionalen irreduziblen stetigen $\mathbb{C}$-Darstellungen, die sogenannten *Galoisdarstellungen*, von G_k und für deren Artinsche L-Reihen, vgl. z.B. [8, 1]. Das eröffnet ein weites Feld, überstrahlt von der sogenannten Langlands Philosophie. Demgegenüber ist das Ziel der vorliegenden Note, wie man bald sehen wird, außerordentlich bescheiden. Dennoch hofft der Verfasser, daß sie in irgendeiner Hinsicht nicht völlig nutzlos ist. Zunächst läßt sich das Klassifikationsproblem vergröbern, indem man die Menge der n-dimensionalen Galoisdarstellungen von G_k in gewisse Aequivalenzklassen einteilt: Zwei n-dimensionale Galoisdarstellungen D, D' von G_k heißen *projektiv aequivalent*, falls eine eindimensionale Galoisdarstellung λ von G_k existiert, so daß D' ähnlich zu $\lambda \otimes D$ ist. Die zu den offenen Untergruppen Ker D bzw. Ker D' von G_k gehörigen Fixkörper L, L' gehören dann wegen Ker $D' \cap$ Ker $\lambda =$ Ker $D \cap$ Ker λ zum gleichen Geschlecht, d.h. es existiert eine endliche abelsche Erweiterung k_0 von k, nämlich der Fixkörper zu Ker λ, so daß $L' \cdot k_0 = L \cdot k_0$. Es entsteht die folgende Frage: Gegeben ist eine n-dimensionale Galoisdarstellung $D: G_k \to GL(n, \mathbb{C})$. Lassen sich Aussagen über den kleinstmöglichen Grad $l(D)$, den eine zum Geschlecht von D gehörige Erweiterung L/k annehmen kann, machen? In der vorliegenden Note soll für den Fall, daß D *primitiv*, d.h. irreduzibel und nicht echt induziert ist, eine Abschätzung für $l(D)$, den sogenannten *Liftungsindex* von D, gegeben werden, die vom Grad n und einer gewissen durch D bestimmten endlichen Primstellenmenge von k abhängt. Die Beschränkung auf primitive Darstellungen erscheint vom Standpunkt der Theorie der Artinschen L-

0021-8693/82/020535–08$02.00/0

Reihen nicht unvernünftig; denn diese verhalten sich ja bekanntlich gegenüber dem darstellungstheoretischen Induktionsprozeß invariant. Aus dem Hauptresultat (4.1) wird sich dann ein gewisser Endlichkeitssatz (4.4) für die projektiven Aequivalenzklassen primitiver Galoisdarstellungen von gegebenem Grad ergeben. Schließlich gestatten die verwendeten Methoden noch eine kleine Anwendung (5.1) auf die Beschreibung der endlichen zentralen Erweiterungen einer vorgegebenen Grundkörpererweiterung K/k, ein Thema, mit dem sich bereits Scholz [8] eingehend befaßt hat.

Ich danke dem Referenten vielmals für Kritik und Rat.

2. Der Kernkőrper der mitgegebenen projektiven Darstellung

Sei $D: G_k \to GL(n, \mathbb{C})$ irgendeine n-dimenionale Galoisdarstellung. Komponiert man D mit der kanonischen Abbildung $\rho: GL(n, \mathbb{C}) \to PGL(n, \mathbb{C})$, so erhält man eine projektive Galoisdarstellung $T: G_k \to PGL(n, \mathbb{C})$ vom Grade n, die nur von der projektiven Aequivalenzklasse von D abhängt. Sei L der Fixkörper zu Ker D und K der zu Ker T. L ist eine K umfassende endliche Galoiserweiterung von k. Mit $H = G(L/k)$, $G = G(K/k)$, $Z = G(L/K)$ bezeichnen wir die entsprechenden Galoisgruppen. Da D irreduzibel ist, stimmt Z nach dem Schurschen Lemma mit dem Zentrum von H überein. Als Untergruppe von $GL(n, \mathbb{C})$ existiert in H nach einem wahlbekannten Resultat von C. Jordan, vgl. z.B. [10, S. 220, Satz 200], ein abelscher Normalteiler vom Index $\leqslant (n!)\, 12^{n(\pi(n+1)+1)}$, wobei $\pi(t)$ die Anzahl der Primzahlen $\leqslant t$ bezeichnet. Ist nun D primitiv, so liegt jeder abelsche Normaliteiler von H nach der Cliffordschen Theorie im Zentrum Z von H. Es ergibt sich also der folgende Hilfssatz.

2.1. Hilfssatz. *Ist D eine primitive Galoisdarstellung von G_k vom Grade n, so gilt für den Kernkörper K der zu D gehörigen projektiven Darstellung die folgende Gradabschätzung*

$$K: k \leqslant (n!)\, 12^{n(\pi(n+1)+1)}.$$

Diese Abschätzung läßt sich in Spezialfällen wesentlich verbessern; z.B. ergibt sich für $n = 2$ aus der bereits von F. Klein aufgestellten Liste von endlichen Untergruppen von $PGL(2, \mathbb{C})$, daß $G \cong A_4$, $\cong S_4$ oder $\cong A_5$ ist, insbesondere ist also für $n = 2$

$$K: k \leqslant 60. \tag{2.2}$$

Aus gruppentheoretischen Resultaten von Dornhoff ergibt sich für den Fall, daß L/k auflösbar ist, eine scharfe Abschätzung für $K: k$. Aber wir gehen nicht näher darauf ein, weil es hier nur auf die Methode ankommen soll.

Sei nun δ: $\mathrm{Hom}(G, PGL(n, \mathbb{C})) \to H^2(G, \mathbb{C}^*)$ der zur exakten Sequenz $1 \to \mathbb{C}^* \to GL(n, \mathbb{C}) \to PGL(n, \mathbb{C}) \to 1$ gehörige Verbindungshomomorphismus und $\bar{f} = \delta(T) \in H^2(G, \mathbb{C}^*)$ die zur projektiven Darstellung $T: G \to PGL(n, \mathbb{C})$ gehörige Kohomologieklasse von zentralen 2-Kozykeln. Nach Haberland [3, 2.4, Proposition 13], ist der Schur-Multiplikator $H^2(G_k, \mathbb{C}^*)$ von G_k trivial. Daraus folgt, daß eine K umfassende endliche Galoiserweiterung L' von k existiert, so daß $\bar{f}$ unter der Inflationsabbildung $H^2(G, \mathbb{C}^*) \to H^2(G(L'/k), \mathbb{C}^*)$ trivial wird. Nach der exakten Sequenz von Hochschild–Serre ist das gleichbedeutend damit, daß $\bar{f}$ im Bild der zugehörigen Transgressionsabbildung $\mathrm{Hom}(G(L'/K), \mathbb{C}^*)^G \to H^2(G, \mathbb{C}^*)$ liegt, so daß also L' von vornherein als zentrale Erweiterung von K/k gewählt werden kann. Die projektive Darstellung T von G läßt sich dann zu einer linearen Darstellung D' van $G(L'/k)$ liften, vgl. [9, Sect. 6]. Daher existiert eine eindimensionale Galoisdarstellung λ von G_k, so daß D' ähnlich zu $\lambda \otimes D$ ist und $L' \cdot k_0 = L \cdot k_0$ gilt, wenn k_0 den Fixkörper zu Ker λ bezeichnet. Es gilt nun, ein L' so zu finden, daß $L': K$ möglichst klein wird.

3. Liften von zentralen Kozykeln

Das Problem stellt sich also so: Sei K/k eine endliche Galoiserweiterung mit Galoisgruppe $G = G(K/k)$ und sei $\bar{f} \in H^2(G, \mathbb{C}^*)$ eine Klasse von zentralen 2-Kozykeln. Finde eine endliche zentrale Erweiterung L von K/k, so daß $L: K$ möglichst klein wird und $\bar{f}$ unter der Inflationsabbildung $H^2(G, \mathbb{C}^*) \to H^2(G(L/k), \mathbb{C}^*)$ trivial wird. Jede zentrale Erweiterung von K/k mit der letzten Eigenschaft heiße *Auflösung* der zyklischen Gruppe $\langle \bar{f} \rangle$. Sei v eine Primstelle von k und w/v eine Fortsetzung von v auf K. Mit G_w bezeichnen wir die Zerlegungsgruppe von w in G. Sei $\bar{f}_w \in H^2(G_w, \mathbb{C}^*)$ die Restriktion von $\bar{f}$ auf G_w. Mit $S = S(\bar{f})$ bezeichnen wir diejenige Menge von Primstellen v von k, für die $\bar{f}_w$, w/v, nicht trivial ist. Es handelt sich um eine endliche Primstellenmenge; denn ihr Komplement enthält die in K unverzweigten Primstellen von k, also fast alle.

3.1. Hilfssatz. *Jede zyklische Untergruppe $A = \langle \bar{f} \rangle$ von $H^2(G, \mathbb{C}^*)$ besitzt eine Auflösung L mit $L: K \leqslant kgV(a_v) \cdot (K: k)$, $v \in S(\bar{f})$, mit $a_v = m_v \cdot m_v'$, wobei $m_v = \exp\langle \bar{f}_w \rangle$, w/v, und m_v' die maximale Ordnung einer in k_v enthaltenen Einheitswurzel von m_v-Potenzordnung bezeichnet.*

Im Beweis von (3.1) werden wir ein einfaches zuerst von Alperin und Kuo angegebenes gruppentheoretisches Resultat benutzen. Es lautet

3.2. HILFSSATZ. *Für jede endliche Gruppe G gilt*: $\exp H^2(G, \mathbb{C}^*) \cdot \exp(G)$ *teilt die Ordnung von G.*

Einen Beweis findet der Leser z.B. in Huppert [5, V, 24.6, S. 640]. Er läßt sich auch schnell erbringen, indem man zunachst auf p-Gruppen reduziert und dann für eine zyklische Untergruppe $I \leqslant G$ von der Ordnung $\exp G$ die Abbildung

$$\begin{array}{ccccc} H^2(G,\mathbb{C}^*) & \xrightarrow{\text{res}} & H^2(I,\mathbb{C}^*) & \xrightarrow{\text{cor}} & H^2(G,\mathbb{C}^*) = G:I \\ & & \| & & \\ & & 1 & & \end{array}$$

betrachtet.

Beweis von 3.1. Sei $m := \exp A$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, läßt sich die Kohomologieklasse $\bar{f}$ durch ein zentrales Faktorensystem $f: G \times G \to \mathbb{C}^*$ repräsentieren, so daß alle Werte von f in der Gruppe W_m der m-ten Einheitswurzeln enthalten sind. Setze $n := kgV(a_v) \cdot (K:k)$, $v \in S(\bar{f})$. Bekanntlich ist m ein Teiler von $K:k$ und damit auch ein Teiler von n. Also gilt $W_m \subset W_n$. Wir bezeichnen mit f auch das Faktorensystem

$$G \times G \xrightarrow{f} W_m \hookrightarrow W_n.$$

Es definiert eine der Schurschen Darstellungsgruppe nachgebildete zentrale Gruppenerweiterung $\tilde{G}$ von G mit Kern W_n. Man rechnet leicht nach, daß $\inf(f): \tilde{G} \times \tilde{G} \to \mathbb{C}^*$ kohomologisch trivial ist. Daher reicht es zu zeigen, daß das durch f definierte Einbettungsproblem lösbar ist: G_k operiert über G trivial auf A. Daher ist die Lokalisierungsabbildung

$$H^2(G_k, A) \to \prod_v H^2(G_{k,\bar{v}}, A),$$

wobei v die Primstellen von k durchläuft und $G_{k,\bar{v}}$ jeweils die Zerlegungsgruppe einer Fortsetzung $\bar{v}$ von v auf $\bar{k}$ bezeichnet, nach Neukirch [7, 4.7, S. 80], injektiv. In dieser Situation läßt sich ein Kriterium von Hoechsmann [4, S. 88 und S. 96], anwenden. Es läuft darauf hinaus zu zeigen, daß für alle i, $1 \leqslant i \leqslant n$, das durch das Faktorensystem f^i vermöge Inflation auf G_k und Restriktion auf $G_{k(\xi^i)}$ – ξ bezeichnet eine primitive n-te Einheitswurzel- entstehende Element $[f^i]$ der Brauergruppe von $k(\xi^i)$ lokal überall trivial ist. Sei $v \notin S(\bar{f})$. Dann existiert eine Funktion $\alpha: G_w \to \mathbb{C}^*$, w/v, so daß $f_w = \delta\alpha$. Wegen $f^m = 1$ ist α^m ein Charakter von G_w. Daher ist $\alpha^{m \cdot \exp G} = 1$. Nach (3.2) sind daher alle Werte von α^i in $k_v(\xi^i)$ enthalten, und $[f^i]$ ist somit an der Stelle v trivial. Sei nun $v \in S(\bar{f})$. Aus Buhler [1, S. 16], ergibt sich die Existenz einer Auflösung $\tilde{K}_w$, w/v, der Untergruppe

$\langle \bar{f}_w \rangle \leqslant H^2(G_w, \mathbb{C}^*)$ mit $\tilde{K}_w : K_w \leqslant a_v$. Daher existiert eine Funktion α: $G(\tilde{K}_w/k_v) \to \mathbb{C}^*$, so daß $\inf(f_w) = \delta\alpha$. Wegen $f^m = 1$ ist α^m ein Charakter von $G(\tilde{K}_w/k_v)$ und damit gilt $\alpha^{m \cdot a_v \cdot \exp G} = 1$, nach (3.2) daher auch $\alpha^n = 1$ und alle Werte von α^i sind in $k(\xi^i)$ enthalten. Daher ist $[f^i]$ an der Stelle $v \in S(\bar{f})$ trivial. Der Beweis ist beendet.

4. Obere Abschätzung für den Liftungsindex

Sei D: $G_k \to GL(n, \mathbb{C})$ eine Galoisdarstellung mit zugehöriger projektiver Darstellung T: $G_k \to PGL(n, \mathbb{C})$. Sei $G_K = G(\bar{k}/K)$ der Kern von T und $G = G(K/k)$. Die exakte Sequenz $1 \to \mathbb{C}^* \to GL(n, \mathbb{C}) \to PGL(n, \mathbb{C}) \to 1$ definiert einen Verbindungshomomorphismus δ: $\mathrm{Hom}(G, PGL(n, \mathbb{C})) \to H^2(G, \mathbb{C}^*)$ und damit eine Kohomologieklasse $\bar{f} = \bar{f}(D) = \delta(T) \in H^2(G, \mathbb{C}^*)$. Sei $S(D) = S(\bar{f})$ die in Abschnitt 3 definierte Primstellenmenge von k.

4.1. Satz. *Ist D primitiv, so gilt für den Liftungsindex $l(D)$ von D die folgende Abschätzung*:

$$l(D) \leqslant kgV(n_v) \cdot [(n!)\, 12^{n(\pi(n+1)+1)}]^2, \qquad v \in S(D),$$

mit $n_v = n \cdot n'_v$, wobei n'_v die maximale Ordnung einer in k_v enthaltenen Einheitswurzel von n-Potenzordnung und $\pi(t)$ die Anzahl der Primzahlen $\leqslant t$ bezeichnet. Für $n = 2$ gilt

$$1(D) \leqslant 3600 \cdot kgV(n_v), \qquad v \in S(D).$$

Beweis. Der Exponent der zu einer projektiven Darstellung T gehörigen Kohomologieklasse $\bar{f}$ teilt den Grad n von T wie Schur mit seinem "Determinantentrick" eindrucksvoll zeigte:

$$\det(T(x))\det(T(y))/\det(T(xy)) = f(x, y)^n.$$

Die Behauptung für allgemeines n ergibt sich daher aus (2.1) und (3.1).

4.2. Folgerung. *Ist D primitiv und $S(D) = \varnothing$, dann gilt*

$$l(D) \leqslant [(n!)\, 12^{n(\pi(n+1)+1)}]^2$$

bzw. im Fall $n = 2$

$$1(D) \leqslant 3600.$$

Auffallend ist, daß im Sonderfall $S(D) = \varnothing$ die Abschätzung für $l(D)$ nur vom Grad n abhängt. Dieser Fall ist nicht völlig aus der Luft gegriffen; nach

A. Scholz läßt sich nämlich jede endliche Gruppe als Galoisgruppe einer unverzweigten Galoiserweiterung K/k von Zahlkörpern realisieren. Der Fall $S(D) = \varnothing$ tritt auch ein, wenn $\bar{f}(D)$ zum Kern $\mathscr{K}(K/k)$ der Lokalisierungsabbildung

$$H^2(G, \mathbb{C}^*) \to \coprod_{\substack{w/v \\ v \text{ Primstelle von } k}} H^2(G_w, \mathbb{C}^*)$$

gehört. Insbesondere gilt dann für K/k nicht der Hassesche Normensatz; denn $\mathscr{K}(K/k)$ ist nach Tate [2, S. 198], isomorph zum sogenannten Zahlknoten

$$\mathscr{K}(K/k) = \frac{\{a \in k^* \mid a \text{ ist lokal überall Norm in } K\}}{\{a \in k^* \mid a \text{ ist globale Norm in } K\}}.$$

Im Fall $n = 2$ hat $H^2(G, \mathbb{C}^*)$ stets die Ordnung 2. Daher läßt sich sagen

4.3. Folgerung. *Ist $n = 2$ und gilt für K/k nicht der Hassesche Normensatz, so ist*

$$l(D) \leqslant 3600.$$

Es soll nicht verschwiegen werden, daß sich die angegebenen Abschätzungen bei Wahl spezieller Grundkörper k zum Teil verbessern lassen.

Ist S eine endliche Primstellenmenge von k, so gibt es nach der Klassenkörpertheorie unterhalb eines gegebenen Grades nur endlich viele außerhalb S unverzweigte Erweiterungen. Aus (4.1) ergibt sich daher

4.4. Folgerung. *Ist S eine endliche Primstellenmenge von k, so gibt es nur endlich viele projektive Aequivalenzklassen primitiver außerhalb S unverzweigter Galoisdarstellungen von G_k von vorgegebenem Grad.*

5. Geschlechter von zentralen Erweiterungen

Sei $K \subset \bar{k}$ eine endliche Galoiserweiterung von k mit Galoisgruppe $G = G(K/k)$. Zwei endliche zentrale Erweiterungen L, L' von K/k heißen vom gleichen Geschlecht, wenn eine endliche abelsche Erweiterung $k_0 \subset \bar{k}$ von k existiert, so daß $L \cdot k_0 = L' \cdot k_0$. Es gilt der folgende Satz.

5.1. Satz. *Die Geschlechter von endlichen zentralen Erweiterungen von*

K/k entsprechen bijektiv den Untergruppen des Schur-Multiplikators $H^2(G, \mathbb{C}^*)$ von G. Gilt für K/k der Hassesche Normensatz, so sind zwei Geschlechter von zentralen Erweiterungen von K/k genau dann gleich, wenn für alle Primstellen v von k, die in K verzweigen, die zugeordneten lokalen Geschlechter von zentralen Erweiterungen von K_w/k_v, w/v, übereinstimmen. Jedes Geschlecht von zentralen Erweiterungen von K/k läßt sich durch eine zentrale Erweiterung L von K/k mit der Eigenschaft

$$L: K \leqslant (\underset{\substack{v \\ \text{verzweigt}}}{kgV}(e_v) \cdot (K:k))^{\mathrm{Rank}(H^2(G, \mathbb{C}^*))}$$

repräsentieren.

Dabei ist $e_v = m_v \cdot m_v'$, wobei $m_v = \exp H^2(G_w, \mathbb{C}^*)$, w/v, und m_v' die maximale Ordnung einer in k_v enthaltenen Einheitswurzel von m_v-Potenzordnung bezeichnet.

Der Verfasser plant, diesen Satz in einer künftigen Arbeit in einen allgemeinen Zusammenhang zu stellen. Deshalb und um die Darstellung nicht zu lang werden zu lassen, geben wir nur eine kurze Beweisskizze: Die erste Aussage ergibt sich aus der Hochschild–Serre Sequenz, die wegen $H^2(G_k, \mathbb{C}^*) = 1$ die folgende Gestalt annimmt:

$$1 \to \hat{G} \xrightarrow{\text{inf}} \hat{G}_k \xrightarrow{\text{res}} \hat{G}_K^G \xrightarrow{\tau} H^2(G, \mathbb{C}^*) \to 1$$

Hier bezeichnet $(\cdots)\hat{}$ das Pontrjagin-Dual. Der zweite Teil ergibt sich aus der Tateschen kohomologischen Deutung des Zahlknotens, vgl. Abschnitt 4. Die Abschätzung schließlich erhält man mit Hilfe von (3.1).

Literaturverzeichnis

1. J. P. Buhler, Icosahedral Galois representations, "Lecture Notes in Mathematics No. 654," Springer-Verlag, Berlin/Heidelberg/New York, 1978.
2. J. W. S. Cassels and A. Fröhlich, "Algebraic Number Theory," Academic Press, London/New York, 1967.
3. K. Haberland, "Galois Cohomology of Algebraic Number Fields," VEB Deutscher Verlag der Wissenschaften, Berlin, 1978.
4. K. Hoechsmann, Zum Einbettungsproblem, *Crelle J.* (*J. Reine Angew. Math.*) **229** (1968), 81–106.
5. B. Huppert, "Endliche Gruppen I," Springer-Verlag, Berlin/Heidelberg/New York, 1967.
6. L. V. Kuzmin, Homology of profinite groups, Schur multiplicator and class field theory, *Izv. Akad. Nauk SSSR Ser. Mat.* **33** (1969), 1220–1254 [Russian]; *Math. USSR Izv.* **3** (1969), 1149–1181. [Engl. Transl.]

7. J. Neukirch, Über das Einbettungsproblem der algebraischen Zahlentheorie, *Invent. Math.* **21** (1973), 59–116.
8. A. Scholz, Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen II, *Crelle J.* (*J. Reine Angew. Math.*) **182** (1940), 217–234.
9. J. P. Serre, Modular forms of weight one and Galois representations, *in* "Algebraic Number Fields" (A. Fröhlich, Ed.), Academic Press, New York/London, 1977.
10. A. Speiser, "Die Theorie der Gruppen von endlicher Ordnung, 4-te Auflage," Birkhäuser Verlag, Basel und Stuttgard, 1956.